AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

LISTING OF CLAIMS

Claims 1-6 (cancelled)

7. (currently amendment) A restricted data format method for a network infrastructure copy protection system, comprising:

receiving a digital content file for transmission across a distributed computer network;

examining data comprising the content file to determine whether the content file includes a restricted data format, the examining performed within the distributed computer network;

transmitting the content file when data comprising the content file does not include the restricted data format; and

blocking transmission of the content file when data comprising the content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the content file to a receiver.

8. (original) The method of Claim 7 wherein the restricted data format includes MP3 data formats.

9. (original) The method of Claim 7 wherein the restricted data format includes MPEG video data formats.

10. (original) The method of Claim 7 wherein the restricted data format includes Word Document formats.

11. (original) The method of Claim 7 wherein the distributed computer network is the Internet.

12. (original) The method of Claim 7 wherein the examining is performed by a plurality of routers within the distributed computer network.

13. (original) The method of Claim 7 wherein the examining is performed by a plurality of cache engines within the distributed computer network.

14. (canceled)

15. (canceled)

16. (canceled)

17. (currently amendment) A network infrastructure protection method for detecting and denying transmission of restricted data formats, comprising:

receiving a content file for transmission across a distributed computer network;

using at least one router configured to log digital signatures related to the content file, examining data comprising the content file to determine whether the content file comprises a restricted data format, wherein the content file is free of a digital signature, the examining performed within the distributed computer network;

transmitting the content file when the data comprising the content file does not include the restricted data format; and

blocking the transmission of the content file when the data comprising the content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the content file to a receiver.

18. (previously presented) The method of Claim 17 wherein the restricted data format is an MP3 data format.

19. (previously presented) The method of Claim 17 wherein the restricted data format is an MPEG video data format.

20. (cancelled)

21. (new) A network device comprising:

one or more network interfaces;

computer readable memory units connected to said bus;

one or more processors coupled to said bus said computer readable memory units for executing a digital signature method for a network infrastructure copy protection system, comprising:

applying a digital signature to a digital content file;

examining the content file to determine whether the content file includes the digital signature, wherein the examining is performed within a distributed computer network;

transmitting the content file when the content file includes the digital signature;

blocking transmission of the content file when the content file does not include the digital signature to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the content file to a receiver; and

blocking transmission of the content file when the data comprising the content files is a restricted data format to prevent unauthorized downloading of copyrighted material.

22. (new) The device of Claim 21 wherein the digital signature is configured to identify the sender of the digital content file.

23. (new) The device of Claim 21 wherein the digital signature applied to the content file within the distributed computer network is logged when the content file is transmitted across the distributed computer network.

24. (new) The device of Claim 21 wherein the distributed computer network is the Internet.

25. (new) The device of Claim 21 wherein the examining is performed by a plurality of routers within the distributed computer network.

26. (new) The device of Claim 21 wherein the examining is performed by a plurality of cache engines within the distributed computer network.

27. (new) A network device comprising:

one or more network interfaces;

computer readable memory units connected to said one or more network interfaces;

one or more processors coupled to said bus said computer readable memory units for executing a method for detecting and denying transmission of restricted data formats, comprising:

receiving a content file for transmission across a distributed computer network;

using at least one router configured to log digital signatures related to the content file, examining data comprising the content file to determine whether the content file comprises a restricted data format, wherein the content file is free of a digital signature, the examining performed within the distributed computer network;

transmitting the content file when the data comprising the content file does not include the restricted data format; and

blocking the transmission of the content file when the data comprising the content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the content file to a receiver.

28. (new) The device of Claim 27 wherein the restricted data format is an MP3 data format.

29. (new) The device of Claim 27 wherein the restricted data format is an MPEG video data format.

30. (new) A restricted data format system for a network infrastructure copy protection system, comprising:

means for receiving a digital content file for transmission across a distributed computer network;

means for examining data comprising the content file to determine whether the content file includes a restricted data format, the examining performed within the distributed computer network;

means for transmitting the content file when data comprising the content file does not include the restricted data format; and

means for blocking transmission of the content file when data comprising the content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the content file to a receiver.

31. (new) A network infrastructure protection system for detecting and denying transmission of restricted data formats, comprising:

means for receiving a content file for transmission across a distributed computer network;

means for using at least one router configured to log digital signatures related to the content file, examining data comprising the content file to determine whether the content file comprises a restricted data format, wherein the content file is free of a digital signature, the examining performed within the distributed computer network;

means for transmitting the content file when the data comprising the content file does not include the restricted data format; and

means for blocking the transmission of the content file when the data comprising the content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the content file to a receiver.